DIR Cybersecurity Insight Newsletter

March FY2015 | DIR OCISO | DIRSECURITY@DIR.TEXAS.GOV

Contents

2015 Information Security Forum Coming Soon!

The *2015 Information Security Forum* (ISF) is just around the corner, and we are looking for meaningful content to add to the conference! This year, the ISF will be a two-day event held at the Palmer Events Center. There will be multiple tracks and break-out sessions on day one and workshops on day two.

If you have recently completed a project or have important security improvements or achievements, we want to hear from you! We have extended our deadline for the Call for Presentations. The new deadline for presentation submissions is Friday- March 13.

Click here to submit a presentation.

Registration for the 2015 ISF will open on Friday- March 20.

Incident Response – Luck or Preparation?

As St. Patrick's Day approaches, we prepare to be pinched if we're not wearing green. We look for a mini invasion of leprechauns and are bombarded with images of four-leaf clovers and other symbols of luck.

As security professionals, we tend to err on the side of paranoia and cynicism. Luck, although it sometimes ends up being a part of the equation, should not be the basis of a sound information security program. Being vigilant and prepared are good qualities to have, not only as an ISO but also as part of a well-rounded security program.

Part of information security is incident management and response. How can an agency ensure they are prepared for the inevitable incident? Depending on luck to get you through an incident is not a solid strategy, but relying on practice, being prepared, and having a good incident response plan can help resolve incidents quickly and with minimal (if any) losses.

The Department of Information Resources (DIR) Office of the Chief Information Security Officer (OCISO) offers monthly tabletop security exercises in partnership with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS). These exercises are available and *free* for agencies and institutes of higher education.

You will need a login ID to the CIAS Learning Management System (LMS), which hosts the instructional classes on how to participate and the exercises themselves. This is a self-service LMS, so anyone in your organization can register for an ID. Click here for the CIAS LMS.

These exercises help you to prepare for different event scenarios to ensure you work through any kinks in your incident response plan and fix any major issues BEFORE a real incident happens. The monthly incidents can be round-table discussions on how to determine severity and escalation levels, how the communication chain works, and which team(s) to involve at which point in the escalation process.

To keep things relatively simple for participants, CIAS created a course that contains all supplemental documents for this initial exercise. Once the participant registers, he or she will see the exercise listed as an available course. The following materials are included in that course:

- Exercise introductory PowerPoint slide deck
- Links to the exercise online videos. These are hosted on a private YouTube channel. Click on *Course Description* to see these links.
- After Action Report/Improvement Plan template
- Online Exercise After Action Report/Improvement Plan Debrief to be sent to DIR
- Exercise Participant Message Worksheet
- Exercise Development Guide (completed for this exercise)

As the custodian of this program, DIR depends on feedback from the community to determine the program's effectiveness and to ensure that we make adjustments that fit your needs. Sending a completed Improvement Plan Debrief template back to DIR gives us the feedback we need to continuously improve the exercises. The more templates we receive, the more effective this program is for the state of Texas. You can send completed templates to DIRsecurity@dir.texas.gov.

Taking advantage of these exercises can help to ensure that your incident response plan and practices are based on preparation, dedication, and vigilance – instead of a four-leaf clove

Network Security Operations Center (NSOC) Updates

In February 2015, the DIR Network Security Operations Center (DIR NSOC) in conjunction with the OCISO created and launched the State of Texas compartment of the Homeland Security Information Network (HSIN) portal.

This portal, hosted by the Department of Homeland Security, provides a means for sharing critical statewide infrastructure news, alerts, and other information in a secure manner.

The NSOC will use the HSIN site for several purposes, including:

- Hosting the Statewide Security Operations (SSO) meetings
- Posting new threat intelligence or indicators of compromise
- Sharing current lists of blocked domains and IP addresses
- Posting documents or polices that are relevant to the SSO group
- Establishing private chat rooms to discuss incidents that may require attention

The chat room feature is a great way to discuss and share information regarding incidents that may involve multiple parties. As the host, we can invite whomever may be needed to address a specific incident and use a separate "virtual" meeting room with confidence that HSIN members are connecting to the hosting room securely.

The HSIN site employs two-factor authentication and will be updated on a weekly basis at minimum. The site is still new, and development continues as we add content and functionality. All SSO members were issued a nomination form to create a HSIN account at the last meeting. A HSIN account will not only ensure you can connect for the monthly SSO meetings but will also give you access to the information listed above.

If you have any questions about HSIN membership, or if you are interested in joining the SSO group, please contact Mac Cole.
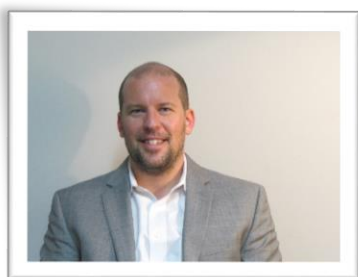
Jeremy A. Wilson
DIR Security Operations Center Manager

Information Security Officer Spotlight

Dan Basile, CISSP-
Information Security Officer
Texas A&M Health Science Center

What is your professional history?
I started straight out of high school running QA tests on risk assessment software for Symantec. From there I moved to Rackspace and became a Data Center Manager. I moved to College Station in 2004 and worked several jobs before ending up at Texas A&M where I worked for a few different departments. About five years ago I came to the Health Science Center.

How did you come to the security field?
I started working on risk assessment and vulnerability assessment software. I took a break from security after that, but after moving to the Health Science Center I took the role of Network Security Engineer which later turned into ISO.

Tell us how information security has changed since you started in your role.
Information Security really hasn't changed that much in the grand scheme of things. It is still about assigning risk and the remediation of risk. On the technical side though, the visibility that is possible now is incredible and just getting better.

Who are your users/customers, and what is one of the most challenging areas for you?
My users are all medical professionals. We work a great deal with protected health information. Getting the proper agreements in place to allow secure data sharing can be challenging.

How did you learn about Texas A&M?
Both of my parents are Aggies, so I learned about Texas A&M at a very young age.

What do you like best of your job?
I enjoy that every day is different. I can see the impacts of my work in many places, and that is very rewarding.

What other career would you have liked to pursue?
Looking back, this has really been the best career for me, and

I have always had a passion for technology. Some days though I think that welding would have been a nice trade.

Tell us about your most proud accomplishment.
I am most proud of my two kids. They impress me every day.

Top 3 life highlights?
The births of my two boys and meeting my wife.

Where did you grow up?
My dad was in the Navy so we moved around when I was young. We settled for a while in Yoakum, TX, but I spent several years in San Antonio as well.

What are your hobbies?
I homebrew beer and I enjoy working on things around the house.

People would be surprised to know that you…
Are a fan of John Wayne movies.

Favorite line of a movie?
"Badges? We don't need no stinkin' badges!"

Are you messy or organized?
Messy, but I know where things are usually.

Favorite travel spot?
I have always enjoyed my time at the state parks in Texas. I haven't found one I didn't like.

What was the last book you read?
I just finished Wool by Hugh Howey.

Which CD do you have in your car?
This morning it was "They Might be Giants –Here Comes Science" and "The Best of Johnny Cash"

If you could interview one person (dead or alive) who would it be?
It would be interesting to speak to Whitfield Diffie and Martin Hellman. Their method of public key encryption changed the method of secure communication overnight. In the information world it was revolutionary.

If you had to eat one meal, every day for the rest of your life, what would it be?
Tacos – it doesn't get much better.

Least favorite food?
Ranch dressing and mac and cheese.

Describe what you were like at age 10.
I was very curious and read quite a few books. With an engineer and geologist for parents I was encouraged to explore and create.

What is one thing you couldn't live without?
My family.

What is your hidden talent?
I like to think I'm a decent handy man.

What would be your advice for a new security professional?
Don't be afraid of telling people no. Not everyone knows or cares about how important security is, and you need to be the guidepost.

Program Updates

Texas InfoSec Academy:

Texas Security Policy & Assurance Course to be Offered Soon

The InfoSec Academy will soon be offering the Texas Security Policy & Assurance course. CISOs and ISOs of state agencies and institutions of higher education are required to take this course. Designed to prepare attendees to apply the Texas rules regarding information security within their agencies, this course will cover Texas Rules and Regulations, data classification, the Texas Cybersecurity Framework, agency security plans, and reporting requirements.

The Texas Security Policy & Assurance course will be offered five times in a classroom setting between April and May. The schedule and registration information will be released soon.

Click here for more information about the InfoSec Academy course tracks.

InfoSec Academy login:

https://infosecacademy.dir.texas.gov/

If you have any questions about the Texas InfoSec Academy, email infosecacademy@dir.texas.gov or call Michele Elledge at 512-475-0419.

Insight from our Texas Interim CISO

February was an interesting time for the security community. We saw the President of the United States discuss cybersecurity at length and trust undermined by a private sector blunder. These two items highlight the challenges we face protecting both the information the citizens of Texas entrust us with and our own personally identifying information.

On February 13, President Obama spoke at the Cybersecurity and Consumer Protection Summit, outlining the problem:

"…it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm. The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops. The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security.[1]"

Eddie Block
Interim CISO Texas

The President is proposing a Consumer Privacy Bill of Rights to ensure that consumers are alerted in a timely manner if their information is breached and a Student Digital Privacy Act to protect students' data from being farmed for marketing. He is promoting sharing between the government and private sector and establishing a Cyber Threat Intelligence Integration Center.

Obviously these efforts are still being formed and we will have to wait to judge their impact. Each of these efforts, though, centers on trust. The most powerful person in the free world has to propose laws to ensure that companies and marketers treat our personal information with care, not as a commodity. Federal action is required to establish enough trust between the government and private sector to share event data.
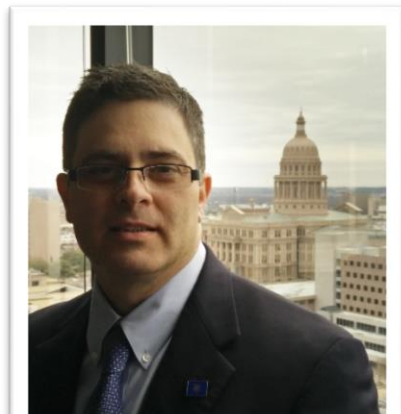
Less than a week after President Obama spoke about the threats posed by nation-state actors and the importance of building secure infrastructures, security researchers reported that Lenovo had bundled software with many of its consumer-grade laptops that circumvented SSL protections.[2] The "Superfish" software has two important components. First, the software intercepts web traffic and injects its own advertisements. While that is seen by many as a violation of the consumers trust, the second component is particularly troubling. The Superfish software created its own SSL certificates which were signed by a root certificate on the laptop. Thus, a visitor to an https website would see their session as encrypted—and therefore "safe"—when the session was actually being monitored.

Aside from the public relations blunder from Lenovo, this software undermines the training that information security professionals have provided to our family, friends, and users. How many of us have told the people in our lives to trust the lock icon in their browsers? Have we drilled into our user community that safe connections would be indicated by a green icon? Did a vendor diminish the trust our users have for our professional opinion?

One of the goals within the OCISO is to ensure that we retain the trust of our agency and higher education partners. As soon as the Superfish issue came to light, we worked with Lenovo to identify all purchases of affected laptops through the DIR cooperative contracts. We are also working closely with our federal partners to ensure that any information sharing initiatives include and support our great state.

Eddie Block

Interim CISO, Texas Department of Information Resources

---

[1] http://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit
[2] http://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html?_r=0

Events

Training and Conferences Around the State

Monthly Security Program Webinar
Identity and Security Intelligence: Bringing them together with SIEM
Date: Tuesday, March 10th, 2015
Time: 2:00 pm CDT
https://attendee.gotowebinar.com/register/8803618443472383234

 2015

Date: Wednesday-Thursday, May 20-21, 2015 |
Time: 8:00 - 4:30
Place: Palmer Events Center
             900 Barton Springs Road
             Austin, Texas 78704

Registration will open March 20.
Visit the website for more information.

2015 Save the Dates

- BSides Austin: March 12 – 13 http://bsidestexas.blogspot.com/p/austin-2013.html
- BSides San Antonio: May 10 http://bsidestexas.blogspot.com/p/san-antonio-april-2013.html
- ISO 27001 summit: May 13 – 14 http://iso27001.com/
- NSA Information Assurance Directorate (IAD)'s Information Assurance Symposium (IAS): June 29 – July 1 DC https://www.fbcinc.com/e/ias/default.aspx
- Blackhat USA: August 1 – 6 https://www.blackhat.com/us-15/
- BSides Las Vegas: August 5 – 6
- Defcon 23: August 6 – 9 https://www.defcon.org/
- LASCON 2015: October 19 – 22
- Dallas Secure World: October 28 – 29, 2015 http://www.secureworldexpo.com/dallas/home

 Feedback, comments, stories, etc.
DIRSecurity@dir.texas.gov

 Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas